AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims:

1.   (Currently Amended) A distributed security system comprising:

a security policy written in a security protocol independent security policy language; and

a plurality of computer devices within the distributed security system comprising at least first and second computer devices which process data in accordance with the security policy of the distributed security system;

wherein the security policy is configurable to be simultaneously implemented for [[a]]the plurality of computer devices within the distributed security system,

wherein the security policy comprises abstract cryptographic objects such that the security policy is implemented independent of a plurality of underlying cryptographic technologies,

wherein at least [[a]]the first computer device within the distributed security system operates on an operating platform that supports at least one security protocol that is different than a security protocol supported by a platform of at least [[a]]the second computer device among the plurality of computer devices, and

wherein the first and the second computer devices process data in accordance with the security policy of the distributed security system, wherein the first computer device performs authentication and processes data in accordance with the security policy according to a first cryptographic technique and the second computer device performs authentication and processes data in accordance with the security policy according to a second cryptographic technique, the first cryptographic technique different from the second cryptographic technique.

2.   (Original) The distributed security system of claim 1, wherein:

the security policy identifies components of the security system.

3.   (Original) The distributed security system of claim 1, wherein: the security policy identifies access rights of the security system.

4.   (Original) The distributed security system of claim 1, wherein:

the security policy language comprises the extensible markup language.

5.   (Original) The distributed security system of claim 1, wherein:

the security policy is configurable.

6.   (Original) The distributed security system of claim 1, wherein:

the security policy language comprises at least some logic-based components.

7.   (Original) The distributed security system of claim 1, wherein:

the security policy language comprises at least some rule-based components.

8.   (Original) The distributed security system of claim 1, wherein:

the security policy language comprises procedural components.

9.   (Original) The distributed security system of claim 1, wherein the computer device is configured with computer-executable instructions to:

receive from a first entity a message formatted in a first protocol; and transmit to a second entity the message formatted in a second protocol that is different from the first protocol.

10.   (Original) The distributed security system of claim 9, wherein the computer device is configured with computer-executable instructions to:

receive from a first entity a message transported with a first transport; and

transmit to the second entity the message using a second transport that is different from the first transport.

11.   (Original) The distributed security system of claim 1, wherein the security policy is implemented with at least one application programming interface.

12.   (Original) The distributed security system of claim 1, wherein the security language includes programming language constructs.

13.　　(Original) The distributed security system of claim 1, wherein the security policy includes an identity service.

14.　　(Original) The distributed security system of claim 1, wherein the security policy includes an admission service.

15.　　(Original) The distributed security system of claim 1, wherein the security policy includes a permission service.

16.　　(Original) The distributed security system of claim 1, wherein the security policy includes a revocation service.

17.　　(Original) The distributed security system of claim 1, wherein the security policy includes a mapping of entities to rights.

18.　　(Original) The distributed security system of claim 17, wherein the security policy further includes a mapping of entities to capabilities.

19.　　(Original) The distributed security system of claim 1, wherein the security policy is configured to invoke external computer-readable instructions.

20.　　(Original) The distributed security system of claim 19, wherein the external computer-readable instructions comprise native processor code.

21.　　(Original) The distributed security system of claim 19, wherein the external computer-readable instructions comprise Java code.

22.　　(Withdrawn) A method of delegating security credentials, the method including:
providing to a second party a first license issued to a first party; and
providing to the second party a second license that allows the second party to use the first

license.

      23.   (Withdrawn) The method of claim 22, wherein the second license is issued by the first party.

      24.   (Withdrawn) The method of claim 22, wherein the second license includes conditions on the use of the first license.

25.   (Withdrawn) A method of transmitting a message between a first party and a second party, the method including:

receiving from the first party a message addressed to the second party, wherein the message is transported with a first transport and formatted in accordance with a first protocol;

determining a transport and protocol required by the second party from a security policy; and

transmitting the message to the second party using the transport and protocol required by the second party.

26.   (Withdrawn) A method of transmitting a secure message between a first party and a second party, the method including:

formatting the message with a markup language; and

inserting a security credential into a header of the message.

27.   (Withdrawn) The method of claim 26, wherein the markup language comprises the extensible markup language.

28.   (Withdrawn) The method of claim 26, wherein the security credential comprises a license.

29.   (Withdrawn) The method of claim 26, wherein the security credential comprises a key.

30.   (Withdrawn) A method of defining a security arrangement between entities of a distributed computing system, the method including:

identifying a portion of a first security policy written in a first security policy language;

identifying a portion of a second security policy written in a second security policy language; and

processing data in accordance with the portion of the first security policy and the portion of the second security policy.

31.   (Withdrawn) The method of claim 30, further including exchanging messages between the entities to negotiate on the identification of the portion of the first security policy and the portion of the second security policy.

32.   (Withdrawn) The method of claim 30, wherein the first security policy language is the same as the second security policy language.

33.   (Currently Amended) A method for utilizing a security policy comprising the steps of:

implementing a security policy written in a security protocol independent security policy language within a distributed computing system,

wherein the security policy comprises abstract cryptographic objects such that the security policy is implemented independent of a plurality of underlying cryptographic technologies,

wherein the distributed computing system comprises at least a first computer device operating on a first operating platform and at least a second computer device operating on a second operating platform that supports at least one security protocol that is different than a security protocol supported by a platform of the first computer device; and

configuring the security policy to allow the first computer device and the second computer device to simultaneously process data in accordance with the security policy of the distributed security system, wherein the first computer device performs authentication and processes data in accordance with the security policy according to a first cryptographic technique and the second computer device performs authentication and processes data in accordance with the security policy according to a second cryptographic technique, the first cryptographic technique different from the second cryptographic technique.

34.   (Currently Amended) A computer readable medium having computer-executable instructions that when executed perform the steps comprising:

applying a security policy within a distributed computing system having at least a first computer device operating on a first operating platform and at least a second computer device operating on a second operating platform that supports at least one security protocol that is different than a security protocol supported by a platform of the first computer device, wherein the security policy is written in a security protocol independent security policy language, wherein the security policy comprises abstract cryptographic objects such that the security policy is implemented independent of a plurality of underlying cryptographic technologies; and

permitting implementing the security policy to be simultaneously implemented for a plurality of computer devices within the distributed security system including at least the first computer device and the second computer device, wherein the first computer device performs authentication and processes data in accordance with the security policy according to a first cryptographic technique and the second computer device performs authentication and processes data in accordance with the security policy according to a second cryptographic technique, the first cryptographic technique different from the second cryptographic technique.